68. An enciphering method according to claim 67, wherein the predetermined bits of the result of the addition are updated with a result of the further addition of the extracted bit.

69. An enciphering method according to claim 68, wherein predetermined bits are selected from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

a6

70. An enciphering method according to claim 46, further comprising the step of transmitting the data enciphered with the cryptographic key to another apparatus via a bus.

71. A deciphering method according to claim 50, wherein a first cryptographic key is produced using one of the first information and the second information, and a second cryptographic key is produced using the other of the first information and the second information, and the enciphered data is first deciphered using the first cryptographic key, the data deciphered using the first cryptographic key is further deciphered using the second cryptographic key.

72. A deciphering apparatus according to claim 71, wherein deciphering using said second cryptographic key is performed by application software for processing the deciphered data.

IN THE ABSTRACT:

Please cancel the present Abstract, and substitute the attached Abstract in its place.

ABSTRACT OF THE DISCLOSURE

The invention provides an enciphering apparatus and method, a deciphering apparatus and method and an information processing apparatus and method by which illegal copying can be prevented with certainty. Data enciphered by a 1394 interface of a DVD player is transmitted to a personal computer and a magneto-optical disk apparatus through a 1394 bus. In the magneto-optical disk apparatus with which a change to a function is not open to a user, the received data is deciphered by a 1394 interface. In contrast, in the personal computer with which a change to a function is open to a user, the enciphered data is deciphered using a time variable key by a 1394 interface, and a result of the decipherment is further deciphered using a session key by an application section.

Docket No. 500.39003X00